(19) Bundesrepublik Deutschland
Deutsches Patent- und Markenamt

(10) **DE 603 13 306 T2** 2007.07.19

(12) # Übersetzung der europäischen Patentschrift

(97) **EP 1 488 577 B1**
(21) Deutsches Aktenzeichen: **603 13 306.1**
(86) PCT-Aktenzeichen: **PCT/CA03/00363**
(96) Europäisches Aktenzeichen: **03 707 963.9**
(87) PCT-Veröffentlichungs-Nr.: **WO 2003/079614**
(86) PCT-Anmeldetag: **18.03.2003**
(87) Veröffentlichungstag der PCT-Anmeldung: **25.09.2003**
(97) Erstveröffentlichung durch das EPA: **22.12.2004**
(97) Veröffentlichungstag der Patenterteilung beim EPA: **18.04.2007**
(47) Veröffentlichungstag im Patentblatt: **19.07.2007**

(51) Int Cl.[8]: ***H04L 12/46*** (2006.01)
H04L 12/24 (2006.01)

(30) Unionspriorität:
365878 P **18.03.2002** **US**

(84) Benannte Vertragsstaaten:
DE, FR, GB

(73) Patentinhaber:
Nortel Networks Ltd., St. Laurent, Quebec, CA

(72) Erfinder:
OULD-BRAHIM, Hamid, Kanata, Ontario K2M 2S8, CA; FEDYK, Donald, Groton, MA 01450, US

(74) Vertreter:
Patentanwälte Wallach, Koch & Partner, 80339 München

(54) Bezeichnung: **RESSOURCENZUTEILUNG MIT HILFE EINES AUTOMATISCHEN ERKENNUNGSVERFAHRENS FÜR PROVIDERKONTROLLIERTE SCHICHT-2 UND SCHICHT-3 VIRTUELLE PRIVATE NETZWERKE**

Beschreibung

Gebiet der Erfindung

[0001] Die vorliegende Erfindung bezieht sich allgemein auf virtuelle private Netzwerke (VPNs) und insbesondere auf eine Technik zur Implementierung einer Ressourcen-Zuteilung zur Implementierung von VPN-Diensten unter Verwendung eines automatischen Erkennungsprozesses zur Konfiguration von einer oder mehreren Schicht-2- und Schicht-3-VPNs.

Hintergrund der Erfindung

[0002] Bei Fehlen eines Vertraulichkeitsmechanismus können schutzwürdige Daten (beispielsweise Passwörter, Kontonummern, private Information, usw.), die über ein Netzwerk übertragen werden, durch unberechtigte Teilnehmer abgefangen werden. Ein Vertraulichkeitsmechanismus, der üblicherweise zum Schutz von Netzwerk-Daten verwendet wird, ist das virtuelle private Netzwerk (VPN). Unter Verwendung spezialisierter Tunnelungs-Protokolle und wahlweise von sicheren Verschlüsselungstechniken kann die Datenintegrität und die Vertraulichkeit in einem VPN aufrechterhalten werden, das ähnlich wie eine dedizierte Punkt-zu-Punkt-Verbindung erscheint.

[0003] Netzwerk-basierte VPNs werden typischerweise durch einen Tunnelungsmechanismus implementiert. Im Allgemeinen kapselt der Tunnelungsmechanismus die Paket-Kopffelder und/oder die Nutzdaten vor der Übertragung des Paketes über einen aufgebauten VPN-Tunnel ein. Als Ergebnis verwendet die Übertragung eines VPN-basierten Paketes lediglich Nicht-Tunnelungs-Information, wie z.B. Internetprotokoll-(IP-)Adressen der Enden der Tunnels, während die schutzwürdigen Daten, wie z. B. die Quellen- und Ziel-IP-Adressen und schutzwürdige Nutzdaten eingekapselt bleiben. Beispiele von Tunnelungsmechanismen schließen die IP/IP-Tunnelung, die generische Router-Einkapselungs-(GRE-)Tunnelung, die IP-Sicherheits-(IP-Sec-)Tunnelung und die Multiprotokoll-Etikettvermittlungs-(MPLS-)Tunnelung ein. Die Konfiguration eines VPN-Tunnels ist typischerweise für die spezielle Art des verwendeten VPN spezifisch.

[0004] Ein typisches Netzwerk-IP-basiertes VPN schließt im Allgemeinen zwei Diensteanbieter-Rand-(PE-)Geräte (beispielsweise einen VPN-fähigen Router) ein, die über eine Serie von Diensteanbieter-Geräten (beispielsweise Router) miteinander verbunden sind, die einen Netzwerk-Backbone bilden, wobei der Netzwerk-Backbone typischerweise ein oder mehrere öffentliche Netzwerke einschließt, wie z.B. das Internet oder ein Weitbereichs-Netzwerk (WAN). Mit jedem PE-Gerät sind ein oder mehrere Kunden-Rand-(CE-)Geräte, wie z.B. eine Arbeitsstation oder ein persönlicher Computer, verbunden. Bei dieser Art von Netzwerk-basierten VPN werden VPN-Tunnels zwischen PE-Geräten anstatt zwischen CE-Geräten aufgebaut. Diese Tunnels, die hier als PE-PE-Tunnels bezeichnet werden, werden typischerweise entweder an der Schicht-2 oder der Schicht-3 des Zwischenverbindungs-(ISO/OSI-)Netzwerk-Modells der Internationalen Normungsorganisation für offene Systeme gebaut. Beispiele von VPN-Mechanismen an der Schicht-2 schließen den virtuellen privaten LAN-Dienst (VPLS) (siehe Waldemar Augustyn et al., „Requirements for Virtual Private LAN Services (VPLS)", Oktober 2002, erhältlich unter <http://www.ietf.org/internetdrafts/draft-ietf-pp-vpn-vpls-requirements-01.txt>) und virtuelle private drahtgebundene Netze (VPW) (siehe Eric Rosen et al., „L2VPN Framework", Februar 2003, erhältlich unter <http://www.ietf.org/internet-drafts/draft-ietf-pp-vpn-12-framework-03.txt>) ein. Beispiele von VPN-Mechanismen auf der Schicht-3 schließen virtuelle Routenführungs-(VR-)basierte Mechanismen ein (siehe Hamid Ould-Brahim et al. „Network based IP VPN Architecture using Virtual Routers", Juli 2002, verfügbar unter <http://www.ietf.org/internet-drafts/draft-ietf-ppvpn-vpn-vr-03.txt>) oder VPNs, die auf der Norm RFC 2547bis beruhen (die in vielen Fällen als BGP/MLPS-basierte VPNs bezeichnet werden). (Siehe Erich Rosen et al., „BGP/MPLS VPNs", verfügbar unter <http://www.ietf.org/internet-drafts/draft-ietf-ppvpn-rfc2547bis-03.txt>, Oktober 2002).

[0005] Unabhängig von dem verwendeten VPN-Mechanismus besteht ein primärer Schritt beim Aufbau eines Netzwerk-basierten VPN in der Bereitstellung von Information über jedes VPN, das auf einem örtlichen PE-Gerät konfiguriert ist, an die verbleibenden PE-Geräte. Eine Anzahl von Mechanismen kann implementiert werden, um diese Verteilung der PE-Information zu erzielen, wie z.B. BGP, Domänen-Namensdienst (DNS), Fernauthentifizierungs-Einwähl-Benutzerdienst (RADIUS) und dergleichen. Derartige Mechanismen sind in der Technik gut bekannt. Nach der Verteilung dieser PE-Information werden typischerweise ein oder mehrere PE-PE-Tunnels teilweise auf der Grundlage von Information aufgebaut, die über einen automatischen VPN-Erkennungsmechanismus empfangen wird.

[0006] Es könnten verschiedene Tunnel-Signalisierungsprotokolle verwendet werden, um VPN-Tunnel aufzubauen und zu unterhalten, wie z.B. das Ressourcen-Reservierungsprotokoll (RSVP) das Ressourcen-Reservierungsprotokoll-Verkehrs-Engineering (RSVP-TE), das Etikett-Verteilungsprotokoll (LBP), das Bedingungs-basierte Routenführungs-LDP (CR-LDP), die asynchrone Übertragungsbetriebsart (ATM), Frame Relay, generische Routenführungs-Einkapselung (GRE), IPSsec und dergleichen.

[0007] Verschiedene Parameter für VPN-Tunnels in konventionellen Schicht-2- und Schicht-3-VPNs werden typischerweise manuell durch den Diensteanbieter konfiguriert. Als Ergebnis ist die Skalierbarkeit derartiger konventioneller VPN-Implementierungen aufgrund der Schwierigkeit beschränkt, die sich aus der manuellen Konfiguration eines komplexen und dynamischen VPN-Systems ergibt, das eine große Anzahl von PE-Geräten aufweist und/oder sich dauernd ändernden Systemanforderungen, wie z.B. eine sich kontinuierlich ändernde Anzahl von Tunnels/VPNs, konstante kontinuierliche Änderungen der Ressourcen, wie z.B. der Bandbreite, Verzögerung und/oder Dienstgüte-(QoS-)Anforderungen und dergleichen aufweist. Weiterhin fehlt diesen konventionellen VPN-Implementierungen allgemein ein definierter Mechanismus, um VPN-Tunnels zu Ressourcen pro VPNs oder pro Satz von VPNs in Beziehung zu setzen, wie z.B. QoS-Profile oder andere Tunnel-spezifische Parameter. Als Ergebnis ist die Flexibilität derartiger konventioneller VPN-Systeme beeinträchtigt, weil das VPN nicht in der Lage ist, in vorhersagbarer Weise auf Änderungen des Bandbreitenbedarfs, der QoS-Anforderungen und dergleichen zu reagieren.

[0008] Im Hinblick auf das Vorstehende würde es wünschenswert sein, eine Technik zur Erleichterung der Konfiguration von VPN-Tunnels auf der Grundlage zumindest teilweise von zugeführten Parametern in einer automatischen Erkennungs-Betriebsweise zu ermöglichen. Insbesondere würde es wünschenswert sein, Ressourcen-Profile, wie z.B. Dienstgüte-(QoS-)Parameter unter Verwendung einer automatischen VPN-Erkennung als Erweiterung zu vorhandenen automatischen Erkennungsmechanismen in einer effizienten und kosteneffektiven Weise zu implementieren.

Zusammenfassung der Erfindung

[0009] Gemäß einem Gesichtspunkt der vorliegenden Erfindung wird ein Verfahren zum Aufbau eines virtuellen privaten Netzwerk-(VPN-)Tunnels zwischen einem ersten Diensteanbieter-Rand-(PE-)Gerät und einem zweiten (PE-)Gerät eines von einem Diensteanbieter bereitgestellten VPN (PPVPN) geschaffen. Das Verfahren umfasst die Ankündigung von zumindest einem Tunnel-basierten Parameter an ein oder mehrere PE-Geräte über einen Netzwerk-Backbone unter Verwendung eines automatischen Erkennungsmechanismus, wobei das eine oder mehrere PE-Geräte zumindest eines der ersten und zweiten PE-Geräte einschließen, und die Konfigurieration eines VPN-Tunnels zwischen den ersten und zweiten PE-Geräten zumindest teilweise auf der Grundlage des zumindest einen Tunnel-basierten Parameters. Ein Computersignal, das in einer Trägerschwingung verkörpert ist, die von einem Computersystem lesbar ist, und die Codierung eines Computer-Programms von Befehlen zur Ausführung eines Computer-Prozesses können zur Durchführung des vorstehenden Verfahrens verwendet werden. Die Erfindung ergibt weiterhin zumindest einen lesbaren Träger zum Speichern eines Computer-Programms von Befehlen, der so konfiguriert ist, dass er von zumindest einem Prozessor lesbar ist, um Befehle an den zumindest einen Prozessor zu liefern, um einen Computer-Prozess zur Durchführung des vorstehenden Verfahrens auszuführen.

[0010] Ein von einem Diensteanbieter bereitgestellte virtuelles privates Netzwerk-(PPVPN-)System wird gemäß einem weiteren Gesichtspunkt der vorliegenden Erfindung geschaffen. Das System umfasst eine automatische Erkennungseinrichtung zur Verteilung von zumindest einem virtuellen privaten Netzwerk-(VPN-)Tunnel-basierten Parameter an zumindest ein erstes und ein zweites Diensteanbieter-Rand-(PE-)Gerät und Tunnel-Signalisierungseinrichtungen zum Konfigurieren eines VPN-Tunnels über einen Netzwerk-Backbone zwischen den ersten und zweiten PE-Geräten zumindest teilweise auf der Grundlage des zumindest einen Tunnel-basierten Parameters.

[0011] Die vorliegende Erfindung wird nunmehr ausführlicher unter Bezugnahme auf Ausführungsbeispiele der Erfindung beschrieben, wie sie in den beigefügten Zeichnungen gezeigt sind. Obwohl die vorliegende Erfindung nachfolgend unter Bezugnahme auf bevorzugte Ausführungsbeispiele beschrieben wird, sollte es verständlich sein, dass die vorliegende Erfindung nicht hierauf beschränkt ist. Der Fachmann, der Zugang zu den vorliegenden Lehren hat, wird zusätzliche Implementationen, Modifikationen und Ausführungsformen sowie andere Anwendungsgebiete erkennen, die in den Schutzumfang der vorliegenden Erfindung fallen, wie sie hier beschrieben und beansprucht ist, und für die die vorliegende Erfindung eine erhebliche Nützlichkeit haben sollte.

[0012] Um ein volles Verständnis der vorliegenden Erfindung zu erleichtern, wird nunmehr auf die beigefügten Zeichnungen verwiesen. Diese Zeichnungen sollten nicht als die vorliegende Erfindung beschränkend ausgelegt werden, sondern sie sollen lediglich Beispiele sein.

[0013] Fig. 1 ist eine schematische Darstellung, die ein von einem Diensteanbieter bereitgestelltes virtuelles privates Netzwerk-(PPVPN-)System erläutert, das einen automatischen VPN-Erkennungsmechanismus gemäß zumindest einer Ausführungsform der vorliegenden Erfindung verwendet.

[0014] Fig. 2 ist ein Ablaufdiagramm, das einen Überblick eines automatischen VPN-Erkennungsmechanismus zum Aufbau und/oder zur Aufrechterhal-

tung eines Diensteanbieter-Rand-zu-Diensteanbieter-Rand-(PE-PE-)Tunnels gemäß zumindest einer Ausführungsform der vorliegenden Erfindung erläutert.

[0015] Fig. 3 ist ein Ablaufdiagramm, das ein Beispiel einer Implementierung eines automatischen VPN-Erkennungsmechanismus nach Fig. 2 in einem RFC2547bis-basierten VPN gemäß zumindest einer Ausführungsform der vorliegenden Erfindung erläutert.

[0016] Fig. 4 ist ein Ablaufdiagramm, das ein Beispiel einer Implementierung des automatischen VPN-Erkennungsmechanismus nach Fig. 2 in einem auf virtueller Routenführung basierenden VPN gemäß zumindest einer Ausführungsform der vorliegenden Erfindung erläutert.

[0017] Fig. 5 ist ein Ablaufdiagramm, das ein Beispiel einer Implementierung des automatischen VPN-Erkennungsmechanismus nach Fig. 2 in einem Schicht-2-VPN unter Verwendung eines virtuellen privaten lokalen Netzwerk-Dienst-(VPLS-)basierten oder VPW-basierten Mechanismus gemäß zumindest einer Ausführungsform der vorliegenden Erfindung erläutert.

Ausführliche Beschreibung von Ausführungsbeispielen

[0018] Die Fig. 1 bis Fig. 5 zeigen verschiedene Beispiele von Implementierungen zur Schaffung von skalierbaren VPN-PE-PE-Tunnels in Schicht-2- oder Schicht-3-PPVPNs unter Verwendung eines automatischen Erkennungsmechanismus. Information bezüglich des Aufbaus und/oder der Konfiguration eines Tunnels zwischen zwei PE-Geräten kann zwischen den PE-Geräten eines Netzwerkes angekündigt oder verbreitet werden. Diese Information kann beispielsweise das gewünschte Tunnel-Signalisierungs-Protokoll, das Dienstgüte-(QoS-)Profil für den Tunnel, den PE-Tunnel-Endpunkt, die Mitgliedschafts-Information, die zu verwendende VPN-Technologie usw. einschließen. In zumindest einer Ausführungsform kann diese Information als eine Erweiterung zu einem konventionellen automatischen Erkennungsmechanismus angekündigt werden, wie er üblicherweise in VPNs verwendet wird, wie z.B. dem Rand-Überleiteinrichtungs-Protokoll (BGP), Verzeichnisdienst-Protokollen (beispielsweise Domänen-Namensdienst (DNS), RADIUS) und dergleichen. Nach der Verteilung dieser Information kann ein Tunnel zwischen den passenden PE-Geräten zumindest teilweise auf der Grundlage der gelieferten Information aufgebaut werden. Alternativ können die PEs einen vorhandenen Tunnel auswählen, der einige oder alle der gelieferten Parameter erfüllt. Durch Implementieren einer automatischen Erkennungstechnik zur Verteilung des QoS-Profils für den Zweck der VPN-Tunnel-Konfiguration und/oder Aufbau-Information kann die Skalierbarkeit des VPN-Systems verbessert werden, weil das QoS-Profil eines Tunnels entsprechend den Anforderungen der VPN-Dienste eingestellt werden kann, wobei die Information zwischen den PEs in einer automatisierten Weise verteilt wird, statt durch eine manuelle Konfiguration, wie bei konventionellen VPN-Systemen, implementiert zu werden.

[0019] Es wird nunmehr auf Fig. 1 Bezug genommen, in der ein Beispiel eines PPVPN-Systems **100** gezeigt ist, das einen Fähigkeits-Erkennungsmechanismus gemäß zumindest einer Ausführungsform der vorliegenden Erfindung implementiert. Bei dem gezeigten Beispiel schließt das PPVPN-System **100** PE-Router **102**, **104** ein, die über einen Netzwerk-Backbone **106** verbunden sind. Obwohl sie hier als VPN-fähige Router beschrieben werden, können die PE-Router **102**, **104** andere geeignete PE-Geräte einschließen, wie z.B. MPLS-/IP-Schicht-2-Vermittlungen. Der Netzwerk-Backbone **106** kann irgendeine Anzahl von Diensteanbieter-Netzwerk-Geräten einschließen, die miteinander unter Verwendung von einer oder mehreren Datenverbindungsstrecken-Typen verbunden sind, wie z.B. IP, ATM, Frame Relay (FR), Zeitmultiplexierung (TDM), Ethernet, optisches Ethernet, und dergleichen.

[0020] Mit jedem PE-Router **102**, **104** sind ein oder mehrere VPN-Segmente verbunden, wie z.B. die VPN-Segmente **142**–**146**, die mit dem PE-Router **102** verbunden sind, und VPN-Segmente **152**–**156**, die mit dem PE-Router **104** verbunden sind. Jedes VPN-Segment **142**–**146**, **152**–**156** kann ein oder mehrere vernetzte Kunden-Rand-(CE-)Geräte sowie Geräte zur Ermöglichung einer Netzwerk-Verbindungsmöglichkeit einschließen, wie z.B. Hubs, Router, Vermittlungen (Switches), Brücken und dergleichen. Wie dies in der Technik verständlich ist, können CE-Geräte irgendeines einer Vielzahl von vernetzten Geräten einschließen, wie z.B. persönliche Computer, Laptops, Arbeitsstationen und dergleichen.

[0021] Allgemein ist jedes VPN-Segment, das mit dem PE-Router **102** verbunden ist, ein Mitglied des gleichen VPN, wie ein VPN-Segment, das mit dem PE-Router **104** verbunden ist, so dass ein VPN zwischen Geräten auf den VPN-Segmenten aufgebaut wird. In dem dargestellten Beispiel sind die VPN-Segmente **142**, **152** Mitglieder des VPN_A, die VPN-Segmente **144**, **154** sind Mitglieder des VPN_B, und die VPN-Segmente **146**, **156** sind Mitglieder des VPN. Obwohl jedes VPN-Segment in Fig. 1 als ein Mitglied eines einzigen VPN dargestellt ist, ist es verständlich, dass ein VPN-Segment ein Mitglied einer Vielzahl von VPNs sein kann. In gleicher Weise kann ein CE-Gerät ein Mitglied einer Vielzahl von VPNs sein und kann daher ein Mitglied von mehr als einem VPN-Segment sein.

[0022] Um Kommunikationen zwischen VPN-Segmenten zu ermöglichen, kann jeder PE-Router **102**, **104** eine VPN-Schnittstelle einschließen, die einem VPN-Segment entspricht. Zur Erläuterung kann der PE-Router **102** VPN-Schnittstellen **122–126** zur Schnittstellenverbindung jeweils mit VPN-Segmenten **142–146** einschließen, und der PE-Router **104** kann VPN-Schnittstellen **132–136** zur Schnittstellenverbindung mit jeweiligen VPN-Segmenten **152–156** einschließen.

[0023] In Abhängigkeit von der verwendeten VPN-Technologie können die VPN-Schnittstellen **122–126**, **132–136** auf irgendeine einer Vielzahl von Arten implementiert werden. Wenn beispielsweise das PPVPN-System **100** ein Schicht-3-VPN unter Verwendung der virtuellen Routenführung (VR) implementiert, so können die VPN-Schnittstellen **122–126**, **132–136** virtuelle Router einschließen, die durch die PE-Router **102**, **104** implementiert sind, um eine virtuelle Routenführung zwischen den CE-Geräten auf den VPN-Segmenten zu schaffen. Die virtuelle Routenführung und virtuelle Router sind dem Fachmann gut bekannt.

[0024] Wenn beispielsweise das PPVPN-System **100** ein Schicht-3-VPN unter Verwendung von RFC2547bis implementiert, so können die VPN-Schnittstellen **122–126**, **132–136** eine virtuelle Routenführung und Weiterleitung (VRF) einschließen, die durch die Router **102**, **104** implementiert wird, um virtuelle Routenführungs- und Weiterleitungstabellen zwischen den CE-Geräten auf den VPN-Segmenten bereitzustellen. RFC2547bis und die virtuelle Routenführung und Weiterleitung sind dem Fachmann gut bekannt.

[0025] Wenn alternativ das PPVPN-System **100** ein Schicht-2-VPW gemäß VPW implementiert (siehe beispielsweise „L2VPN Framework", weiter oben), so können die VPN-Schnittstellen **122–126**, **132–136** eine virtuelle Vermittlungsinstanz (VSI) einschließen, die durch die PE-Router **102**, **104** implementiert ist, um Schicht-2-Anschluss-Schaltungen zwischen den CE-Geräten auf den VPN-Segmenten zu schaffen. Schicht-2-VPNs und virtuelle Vermittlungsinstanzen sind dem Fachmann gut bekannt.

[0026] Weiterhin kann in zumindest einer Ausführungsform der PE-Router **102** eine automatische Erkennungs-(AD-)Komponente **112** und eine Tunnel-Signalisierungs-Komponente **116** einschließen, und der PE-Router **104** kann eine AD-Komponente **114** und eine Tunnel-Signalisierungs-Komponente **118** einschließen. Wie dies nachfolgend ausführlicher erläutert wird, können die Tunnel-Signalisierungs-Komponenten **116**, **118** so ausgebildet sein, dass sie ein oder mehrere VPN-Tunnels **170** zwischen den PE-Routern **102–104** unter Verwendung von einem oder mehreren Tunnel-Signalisierungsmechanismen schaffen, konfigurieren und/oder unterhalten. Beispiele von Tunnel-Signalisierungsmechanismen, die durch die Tunnel-Signalisierungs-Komponenten **116**, **118** implementiert sind, schließen beispielsweise RSVP, RSVP-TE, LDP, CR-LDP und dergleichen ein.

[0027] Eine Anzahl der zugeführten Parameter kann von den Tunnel-Signalisierungs-Komponenten **116**, **118** verwendet werden, um den einen oder mehrere Tunnels **170** zwischen dem PE-Router **102** und dem PE-Router **104** zu schaffen, zu konfigurieren und/oder zu unterhalten. Diese Parameter können beispielsweise den Typ des zu verwendenden Tunnelungsmechanismus (das heißt die Angabe von RSVP-TE oder CR-LDP); das QoS-Profil für jeden Tunnel **170**; die PE-Tunnel-Endpunkte für eine bestimmte VPN-Mitgliedschaft; die zu verwendende VPN-Technologie (beispielsweise Schicht-3-Technologie gegenüber der Schicht-2-Technologie, 2547bis gegenüber virtueller Routenführung usw.) und dergleichen einschließen. Zur Erleichterung der Diskretion wird diese Information insgesamt hier als die VPN-Fähigkeits-Erkennungs-Information (VCDI) bezeichnet.

[0028] In konventionellen PPVPN-Systemen wird diese Information typischerweise manuell an jedem PE-Router für jede VPN-Mitgliedschaft konfiguriert. Bei einer Ausführungsform kann die AD-Komponente **112** jedoch so ausgebildet sein, dass sie diese Information an andere PE-Router auf dem Backbone **106** unter Verwendung eines automatischen Erkennungsmechanismus ankündigt (der nachfolgend ausführlicher beschrieben wird). Die AD-Komponente **112** kann dann die empfangene VCDI-Information an die Tunnel-Signalisierungs-Komponente **116** zur Verwendung bei der Schaffung, dem Unterhalten und/oder dem Konfigurieren des einen oder mehrerer Tunnels **170** liefern, die der VCDI-Information zugeordnet sind.

[0029] Der automatische Erkennungsmechanismus kann in einer eine Vielzahl von Arten implementiert werden. In zumindest einer Ausführungsform kann der automatische Erkennungsmechanismus als eine Erweiterung für konventionelle Informations-Verteilungs-Protokolle implementiert werden, wie z.B. BGP, DNS und RADIUS. Um die Verwendung von BGP zu erläutern, kann die VCDI-Information für jedes der VPN_A, VPN_B und VPN bestimmt und an die PE-Router **102**, **104** jeweils als Profile **162–166** als Teil einer BGP-Aktualisierung (UPDATE) **160** über den Backbone **106** gesandt werden. Bei Empfang der BGP UPDATE **160** können die AD-Komponenten **112**, **114** (die in diesem Fall jeweils BGP-fähig sind) dann die Profile **162–166** ableiten und die VCDI-Information der Profile **162–166** an die Tunnel-Signalisierungs-Komponenten **116**, **118** zur Verwendung bei der Schaffung, dem Unterhalt und/oder der Konfigu-

ration der VPN-Tunnels) liefern, die jedem VPN zugeordnet sind. DNS, RADIUS, und andere Verzeichnisdienst-Protokolle können in einer ähnlichen Weise erweitert werden, um die VCDI an die PE-Router zu verteilen. Entsprechend kann anstelle einer Notwendigkeit einer manuellen Konfiguration der VPN-Tunnels an jedem PE-Router die VPN-Tunnel-Konfigurations-Information (das heißt die VCDI) auf die automatische Erkennungs-Information dadurch aufgesetzt werden, dass das automatische Erkennungs-Protokoll erweitert wird, um die Übertragung der VCDI-Information einzuschließen.

[0030] Unter Bezugnahme auf Fig. 2 wird ein Überblick über ein Beispiel des VPN-Tunnel-Konfigurations-Prozesses gemäß zumindest einer Ausführungsform der vorliegenden Erfindung erläutert. In dem dargestellten Beispiel beginnt der VPN-Tunnel-Konfigurations-Prozess **200** im Schritt **202**, in dem die VCDI-Information für ein vorgegebenes VPN bestimmt werden kann. Die VCDI-Information kann Information bezüglich der Konfiguration von einem oder mehreren VPN-Tunnels zwischen den PE-Routern für das VPN einschließen. Beispielsweise kann die VCDI-Information die PE-Tunnel-Endpunkte, die Gemeinschafts-Routenziele, Ressourcen-Parameter (beispielsweise minimale Bandbreite, maximale Verzögerung, zugelassene Burst-Größe, zugelassene Rate, Jitter, Fehler, Inhaberschaft, physikalische Position, Art des Transportmediums, usw.), Topologie-Information und andere Parameter spezifizieren, die von den Tunnel-Signalisierungsmechanismen verwendet werden, um einen VPN-Tunnel aufzubauen und/oder zu konfigurieren.

[0031] Im Schritt **204** kann die im Schritt **202** gewonnene VCDI-Information an einige oder alle der PE-Router auf dem Backbone angekündigt werden. Die Ankündigung der VCDI-Information schließt bei einer Ausführungsform die Einfügung der VCDI-Information in ein konventionelles Informations-Verteilungs-Protokoll ein. Beispielsweise könnte die VCDI-Information als eine Erweiterung von BGP eingefügt und zwischen PE-Routern unter Verwendung von beispielsweise einer BGP UPDATE-Übertragung übertragen werden. Alternativ könnte die VCDI-Information entsprechend DNS oder RADIUS formatiert und übertragen werden. Sammelsende-basierte Protokolle können ebenfalls erweitert werden, um ein Sammelsenden der VCDI-Information an einige oder alle der PE-Router über den Backbone auszuführen.

[0032] Im Schritt **206** kann bei Empfang der VCDI-Information ein PE-Router mit der Aushandlung der Schaffung eines VPN-(oder pro VPN-)PE-PE-Tunnels auf der Grundlage von zumindest teilweise der empfangenen VCDI-Information beginnen. Wie dies weiter oben erwähnt wurde, ist die Schaffung und Konfiguration eines VPN-Tunnels in der Technik gut bekannt (siehe Hamid Ould-Brahim et al., „Using BGP as an Auto-Discovery Mechanism for Network-Based VPNs", August 2002, verfügbar unter <http://www.ietf.org/internet-drafts/draft-ietf-pp-vpn-bgvpn-auto-03.txt>.

[0033] Bei der Schaffung und Konfiguration des VPN-Tunnels aus der VCDI-Information kann irgendeiner einer Vielzahl von Tunnelungsmechanismen verwendet werden. Beispiele derartiger Mechanismen schließen beispielsweise RSVP-TE, LDP, CR-LDP und dergleichen ein. Nach der Schaffung des VPN-Tunnels können CE-Geräte auf den verschiedenen VPN-Segmenten dann den VPN-Tunnel verwenden, um Daten sicher zwischen den VPN-Segmenten zu übertragen.

[0034] Es wird nunmehr auf die Fig. 3–Fig. 5 Bezug genommen, in denen verschiedene Beispiele von Implementierungen des Prozesses **200** nach Fig. 2 für bestimmte VPN-Technologien gemäß zumindest einer Ausführungsform der vorliegenden Erfindung dargestellt sind. Fig. 3 zeigt ein Beispiel einer Implementierung des Prozesses **200** für ein VPN-System, das ein Schicht-3-VPN unter Verwendung von RFC2547bis implementiert. Fig. 4 zeigt ein Beispiel einer Implementierung des Prozesses **200** für ein VPN-System, das ein Schicht-3-VPN unter Verwendung einer virtuellen Routenführung implementiert. Fig. 5 zeigt ein Beispiel einer Implementierung des Prozesses **200** für ein VPN-System, das ein Schicht-2-VPN unter Verwendung von VPLS oder VFW implementiert. Obwohl Beispiele von Implementierungen des Prozesses **200** für eine Anzahl von VPN-Technologien gezeigt sind, ist der Fachmann unter Verwendung der hier angegebenen Leitlinien in der Lage, den Prozess **200** für verschiedene andere VPN-Technologien zu modifizieren, ohne von dem Grundgedanken oder Schutzumfang der vorliegenden Erfindung abzuweichen.

[0035] In Fig. 3 ist ein Beispiel eines automatischen Erkennungs-Prozesses **300** zur Verteilung von VPN-Tunnel-Konfigurations-Information in einem Schicht-3-PPVPN auf der Grundlage von RFC2547bis gemäß zumindest einer Ausführungsform der vorliegenden Erfindung gezeigt. Nach der Feststellung der betreffenden VCDI-Information (Schritt **202**, Fig. 2) beginnt der Prozess **300** im Schritt **302**, in dem die VCDI-Information, die einem oder mehreren VPN-Tunnels zugeordnet ist, den AD-Komponenten der PE-Router (beispielsweise den AD-Komponenten **112**, **114**, Fig. 1) angekündigt werden kann, wie dies weiter oben erläutert wurde. Wie dies vorstehend erwähnt wurde, wird die VCDI-Information vorzugsweise als eine Erweiterung eines automatischen Erkennungs-Protokolls verteilt, wie z.B. BGP, DNS oder RADIUS. Im Schritt **304** führt die Tunnel-Signalisierungs-Komponente (beispielsweise die Tunnel-Signalisierungs-Komponenten **116**, **118**, Fig. 1) an einem PE-Router eine Aushandlung

mit dem Tunnelungsmechanismus an einem entsprechenden PE-Router aus, um einen oder mehrere VPN-Tunnels auf der Grundlage zumindest teilweise der gelieferten VCDI-Information aufzubauen und zu konfigurieren. Diese Konfiguration kann beispielsweise die Aushandlung der QoS für den VPN-Tunnel, die Einstellung einer minimalen oder maximalen Bandbreite für den VPN-Tunnel, die Angabe des Tunnelungsmechanismus und dergleichen einschließen. Alternativ kann in einer Ausführungsform die Tunnel-Signalisierungs-Komponente einen bereits existierenden VPN-Tunnel auswählen, der einige oder alle der Parameter erfüllt, die in der VCDI-Information angegeben sind.

[0036] Bei der Schaffung und Konfiguration des VPN-Tunnels (oder der Auswahl eines bereits existierenden Tunnels) können virtuelle Routenführungs-Weiterleitungs-(VRF-)Tabellen an jedem PE-Router erzeugt werden. Die Erzeugung der VRF-Tabellen ist in der Technik gut bekannt. Im Schritt **306** können diese VRF-Tabellen dann an dem Backbone unter Verwendung von beispielsweise des BGP exportiert und dann auf die passenden PE-Router zur Verwendung bei der Routenführung von VPN-Verkehr durch den aufgebauten Tunnel verteilt werden.

[0037] Es wird nunmehr auf Fig. 4 Bezug genommen, in der ein Beispiel eines automatischen Erkennungsprozesses **400** zur Verteilung von VPN-Tunnel-Konfigurations-Information in einem Schicht-3-VPN auf der Grundlage der virtuellen Routenführung gemäß zumindest einer Ausführungsform der vorliegenden Erfindung gezeigt ist. Nach der Bestimmung der betreffenden VCDI-Information (Schritt **202**, Fig. 2) beginnt der Prozess **400** im Schritt **402**, in dem VPN-IDs den Endpunkten des aufzubauenden/auszuwählenden Tunnels zugeordnet werden. An diesem Punkt ist es typischerweise nicht erforderlich, die VR-Präfixe/Adressen anzukündigen. Im Schritt **404** wird eine Liste der VPN-IDs in die übrige VCDI-Information eingefügt, und diese Information kann an die AD-Komponenten der PE-Router angekündigt werden (beispielsweise die AD-Komponenten **112**, **114**, Fig. 1), wie dies weiter oben erläutert wurde. Für Implementierungen mit der virtuellen Routenführung wird die VCDI-Information vorzugsweise als eine Erweiterung einer BGP-Multi-Protokoll-Erweiterung (BGP-MP) verteilt. Andere Informations-Verteilungs-Protokolle, wie z.B. DNS, RADIUS und IP-Sammelsendung können verwendet werden. An diesem Punkt kann es passend sein, die VR-Präfixe/Adressen anzukündigen.

[0038] Im Schritt **406** kann der die VCDI-Information empfangende virtuelle Backbone-Router so ausgebildet sein, dass er einen oder mehrere VPN-Tunnels zumindest teilweise auf der Grundlage der gelieferten VCDI-Information aufbaut und konfiguriert. Diese Konfiguration kann beispielsweise die Aushandlung der QoS für den VPN-Tunnel, die Einstellung einer minimalen oder maximalen Bandbreite für den VPN-Tunnel, die Angabe des Tunnelungsmechanismus und dergleichen einschließen. Alternativ kann bei einer Ausführungsform die Tunnel-Signalisierungs-Komponente einen bereits existierenden VPN-Tunnel auswählen, der einige oder alle der Parameter erfüllt, die in der VCDI-Information angegeben sind. Im Schritt **408** kann die VPN-Topologie-Information in einer Weise angekündigt werden, die ähnlich der Ankündigung der VCDI-Information im Schritt **404** ist.

[0039] Es wird nunmehr auf Fig. 5 Bezug genommen, in der ein Beispiel eines automatischen Erkennungsprozesses **500** zur Verteilung von VPN-Tunnel-Konfigurations-Information in einem Schicht-2-PPVPN auf der Grundlage von VPLS oder VPW gemäß zumindest einer Ausführungsform der vorliegenden Erfindung gezeigt ist. Nach der Feststellung der betreffenden VCDI-Information (Schritt **202**, Fig. 2) beginnt der Prozess **500** im Schritt **502**, in dem die einem oder mehreren VPN-Tunnels zugeordnete VCDI-Information den AD-Komponenten der PE-Router angekündigt wird (beispielsweise den AD-Komponenten **112**, **114**, Fig. 1), wie dies weiter oben erläutert wurde. An diesem Punkt kann es unnötig sein, Schicht-2-VPN-Dienste auszutauschen. Wie dies weiter oben erwähnt wurde, wird die VCDI-Information vorzugsweise als eine Erweiterung eines automatischen Erkennungs-Protokolls, wie z.B. BGP, DNS oder RADIUS, verteilt.

[0040] Im Schritt **504** führt die Tunnel-Signalisierungs-Komponente (beispielsweise die Tunnel-Signalisierungs-Komponenten **116**, **118**, Fig. 1) an einem PE-Router eine Aushandlung mit dem Tunnelungsmechanismus an einem entsprechenden Router aus, um einen oder mehrere VPN-Tunnels auf der Grundlage von zumindest teilweise der gelieferten VCDI-Information aufzubauen und zu konfigurieren. Diese Konfiguration kann beispielsweise die Aushandlung der QoS für den VPN-Tunnel, die Einstellung einer minimalen oder maximalen Bandbreite für den VPN-Tunnel, die Angabe des Tunnelungsmechanismus und dergleichen einschließen. Alternativ kann bei einer Ausführungsform die Tunnel-Signalisierungs-Komponente einen bereits existierenden VPN-Tunnel auswählen, der einige oder alle die Parameter erfüllt, die in der VCDI-Information angegeben sind.

[0041] Nach der Schaffung und Konfiguration des VPN-Tunnels (oder der Auswahl eines bereits existierenden Tunnels) können Schicht-2-VPN-Ankündigungen im Schritt **506** erzeugt und unter Verwendung der Backbone-BGP-Komponente (beispielsweise der AD-Komponenten **112**, **114**) im Schritt **508** verteilt werden.

[0042] An diesem Punkt sei bemerkt, dass die Implementierung eines automatischen Erkennungs-VPN-Tunnel-Konfigurations-Prozesses gemäß der vorliegenden Erfindung, wie er vorstehend beschrieben wurde, typischerweise die Verarbeitung von Eingangsdaten und die Erzeugung von Ausgangsdaten in gewissem Ausmaß beinhaltet. Diese Eingangsdaten-Verarbeitung und Ausgangsdaten-Erzeugung kann in Hardware oder Software implementiert werden. Beispielsweise können spezielle elektronische Komponenten in einem Knoten oder ähnlichen und verwandten Schaltungen zur Implementierung einer automatischen Erkennungs-Komponente und einer Tunnel-Signalisierungs-Komponente gemäß der vorliegenden Erfindung verwendet werden, wie dies weiter oben beschrieben wurde. Alternativ können ein oder mehrere Prozessoren, die gemäß gespeicherter Befehle arbeiten, die Funktionen implementieren, die mit der Implementierung eines automatischen Erkennungs-VPN-Tunnel-Konfigurations-Prozesses gemäß der vorliegenden Erfindung verbunden sind, wie dies vorstehend beschrieben wurde. Wenn dies der Fall ist, liegt es innerhalb des Schutzumfanges der vorliegenden Erfindung, dass derartige Befehle auf einem oder mehreren von einem Prozessor lesbaren Medien gespeichert oder an einen oder mehrere Prozessoren über ein oder mehrere Signale übertragen werden.

[0043] Zusammenfassend ist festzustellen, dass die Erfindung eine Technik zur Ressourcen-Verteilung unter Verwendung eines automatischen Erkennungsmechanismus für von Diensteanbietern bereitgestellte virtuelle private Schicht-2- und Schicht-3-Netzwerke ergibt. Bei einem speziellen Ausführungsbeispiel kann die Technik durch ein Verfahren zum Aufbau eines virtuellen privaten Netzwerk-(VPN-)Tunnels zwischen einem ersten Diensteanbieter-Rand-(PE-)Gerät und einem zweiten (PE-)Gerät eines von einem Diensteanbieter bereitgestellten VPN verwirklicht werden. Das Verfahren umfasst die Ankündigung von zumindest einem Tunnel-basierten Parameter an zumindest ein oder mehrere PE-Geräte über einen Netzwerk-Backbone unter Verwendung eines automatischen Erkennungsmechanismus, wobei das eine oder mehrere PE-Gerät zumindest eine der ersten und zweiten PE-Geräte einschließt. Das Verfahren umfasst weiterhin die Konfiguration eines VPN-Tunnels zwischen den ersten und zweiten PE-Geräten zumindest teilweise auf der Grundlage des zumindest einen Tunnel-basierten Parameters.

[0044] Die vorliegende Erfindung ist hinsichtlich ihres Schutzumfanges nicht durch die speziellen vorstehend beschriebenen Ausführungsformen beschränkt. Tatsächlich sind vielfältige Modifikationen der vorliegenden Erfindung zusätzlich zu den hier beschriebenen für den Fachmann aus der vorstehenden Beschreibung und den beigefügten Zeichnungen ersichtlich. Daher sollen derartige Modifikationen in den Schutzumfang der folgenden beigefügten Ansprüche fallen. Weiterhin wird, obwohl die vorliegende Erfindung hier in dem Zusammenhang mit einer bestimmten Implementierung in einer bestimmten Umgebung für einen speziellen Zweck beschrieben wurde, der Fachmann erkennen, dass die Nützlichkeit der Erfindung nicht hierauf beschränkt ist, und dass die vorliegende Erfindung in vorteilhafter Weise in irgendeiner Anzahl von Umgebungen für irgendeine Anzahl von Zwecken implementiert werden kann.

Patentansprüche

1. Verfahren zum Aufbau eines virtuellen privaten Netzwerk-, VPN-, Tunnels (**170**) zwischen einem ersten Diensteanbieter-Rand-PE-Gerät (**102**) und einem zweiten PE-Gerät (**104**) eines von einem Diensteanbieter bereitgestellten VPN, PPVPN, (**100**), mit den folgenden Schritten:
Ankündigen von zumindest einem Tunnel-basierten Parameter an eines oder mehrere PE-Geräte über einen Netzwerk-Backbone (**106**) unter Verwendung eines automatischen Erkennungsmechanismus, wobei das eine oder die mehreren PE-Geräte zumindest eines der ersten und zweiten PE-Geräte einschließen; und
Konfigurieren eines VPN-Tunnels zwischen den ersten und zweiten PE-Geräten zumindest teilweise auf der Grundlage des zumindest einen Tunnel-basierten Parameters.

2. Verfahren nach Anspruch 1, bei dem der automatische Erkennungsmechanismus einen von folgenden Mechanismen einschließt: einen Rand-Überleiteinrichtungs-Protokoll-, BGP-, basierten Mechanismus; einen Domänen-Namensdienst-, DNS-basierten Mechanismus; und einen Fernauthentifizierungs-Einwähl-Benutzerdienst-, RADIUS-, basierten Mechanismus.

3. Verfahren nach Anspruch 2, bei dem der zumindest eine Tunnel-basierte Parameter an das eine oder die mehreren PE-Geräte als eine Erweiterung eines automatischen Erkennungs-Protokolls verteilt wird.

4. Verfahren nach Anspruch 1, bei dem die Konfiguration des VPN-Tunnels das Konfigurieren des VPN-Tunnels unter Verwendung von zumindest einem Tunnel-Signalisierungsmechanismus einschließt.

5. Verfahren nach Anspruch 4, bei dem der zumindest eine Tunnel-Signalisierungsmechanismus einen von folgenden Mechanismen einschließt: einen Ressourcen-Reservierungs-Protokoll-, RSVP-, basierten Mechanismus; einen Ressourcen-Reservierungs-Protokoll-Verkehrsauslegungs-, RSVP-TE-, basierten Mechanismus; einen Etikettverteilungs-Protokoll-, LDP-, basierten Mechanismus; und

einen Bedingungs-basierten Routenführungs-, LDP-CR-LDP-, basierten Mechanismus.

6. Verfahren nach Anspruch 1, bei dem der zumindest eine Tunnel-Parameter einen von folgenden Parametern einschließt: einen Typ des Tunnelungsmechanismus; zumindest einen PE-Tunnel-Endpunkt; zumindest ein Gemeinschafts-Routen-Ziel; Topologie-Information; und zumindest einen Ressourcen-Parameter.

7. Verfahren nach Anspruch 6, bei dem zumindest eine Ressourcen-Parameter einen von folgenden Parametern einschließt: minimale Bandbreite; maximale Verzögerung; vereinbarte Burst-Größe; vereinbarte Rate; Jitter; Fehler; Inhaberschaft; physikalische Position und Transportmedium.

8. Verfahren nach Anspruch 1, bei dem die Konfiguration des VPN-Tunnels die Auswahl eines bereits existierenden VPN-Tunnels einschließt, wobei der bereits existierende VPN-Tunnel zumindest einen Tunnel-Parameter erfüllt.

9. Von einem Diensteanbieter bereitgestelltes virtuelles privates Netzwerk-, PPVPN-, System, mit:
automatischen Erkennungseinrichtungen zur Verteilung von zumindest einem virtuellen privaten Netzwerk-, VPN-, Tunnel-basierten Parameter an zumindest ein erstes und ein zweites Diensteanbieter-Rand-PE-Gerät (**102**, **104**); und
Tunnel-Signalisierungseinrichtungen zum Konfigurieren eines VPN-Tunnels (**170**) über einen Netzwerk-Backbone (**106**) zwischen den ersten und zweiten PE-Geräten zumindest teilweise auf der Grundlage des zumindest einen Tunnel-basierten Parameters.

10. System nach Anspruch 9, bei dem die automatische Erkennungseinrichtung 1 so ausgebildet ist, dass sie den zumindest einen Tunnel-basierten Parameter als eine Erweiterung von zumindest einem automatischen Erkennungs-Protokoll verteilt.

11. System nach Anspruch 10, bei dem das automatische Erkennungs-Protokoll eines der folgenden Protokolle umfasst: einen Rand-Überleitungseinrichtungs-Protokoll-, BGP-, basierten Mechanismus; einen Domänen-Namensdienst-, DNS-, basierten Mechanismus; und einen Fernauthentifizierungs-Einwähl-Benutzerdienst-, RADIUS-basierten Mechanismus.

12. System nach Anspruch 9, bei dem die Tunnel-Signalisierungseinrichtung einen von folgenden Mechanismen einschließt: einen Ressourcen-Reservierungs-Protokoll-, RSVP-, basierten Mechanismus; einen Ressourcen-Reservierungs-Protokoll-Verkehrsauslegungs-, RSVP-TE-, basierten Mechanismus; einen Etikettverteilungs-Protokoll-, LDP-, basierten Mechanismus; und einen Bedingungs-basierten Routenführungs-, LDP-CR-LDP-, basierten Mechanismus.

13. System nach Anspruch 9, bei dem der zumindest eine Parameter einen von folgenden Parametern einschließt: einen Typ des Tunnelungsmechanismus; zumindest einen PE-Tunnel-Endpunkt; zumindest ein Gemeinschafts-Routenziel; Topologie-Information; und zumindest einen Ressourcen-Parameter.

14. System nach Anspruch 13, bei dem der zumindest eine Ressourcen-Parameter einen von folgenden Parametern einschließt: minimale Bandbreite; maximale Verzögerung; vereinbarte Burst-Größe; vereinbarte Rate; Jitter; Fehler; Inhaberschaft; physikalische Position und Transportmedium.

15. System nach Anspruch 10 mit:
dem Netzwerk-Backbone; und
den ersten und zweiten PE-Geräten, die jeweils betriebsmäßig mit dem Netzwerk-Backbone verbunden sind.

Es folgen 5 Blatt Zeichnungen

Anhängende Zeichnungen

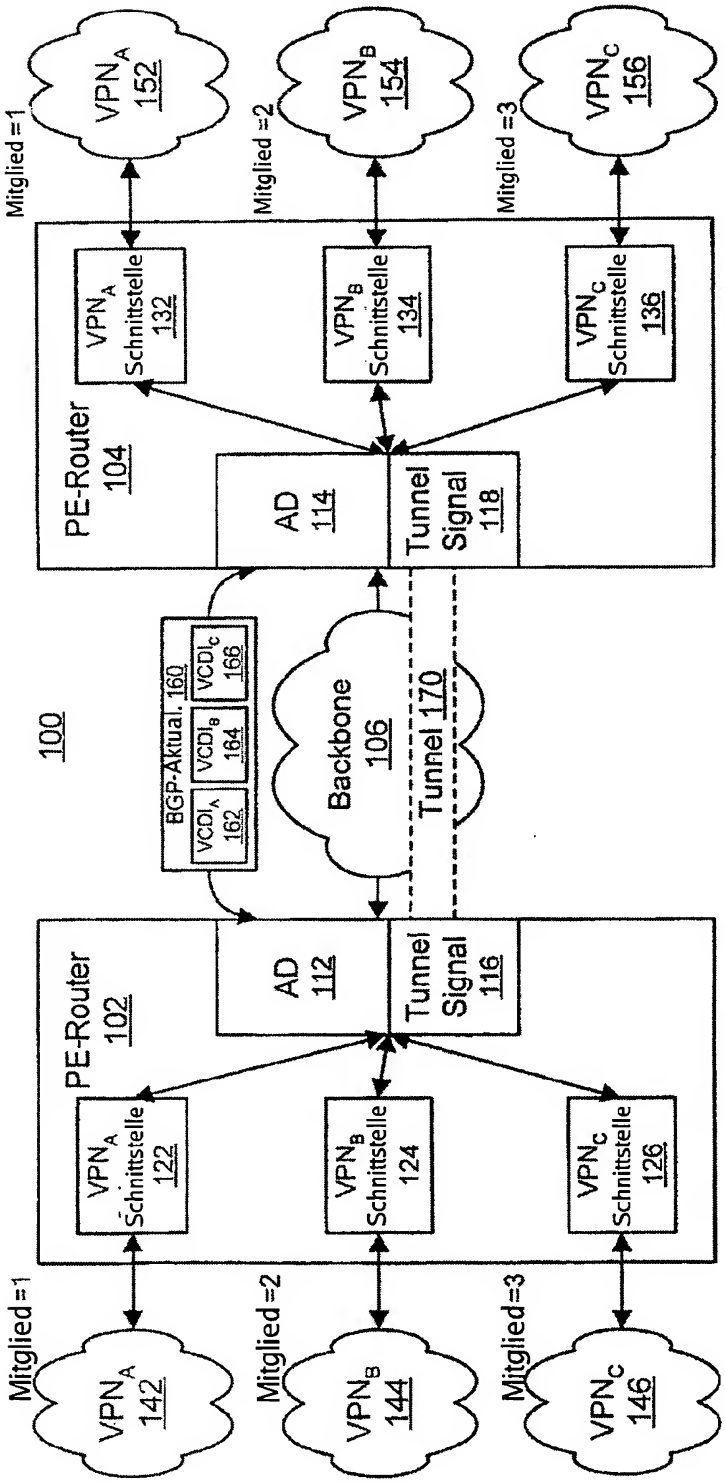

Fig. 1

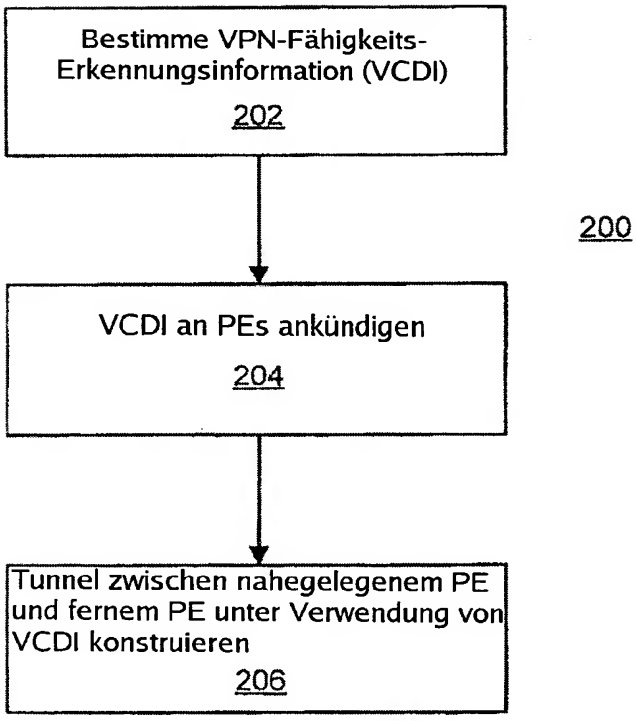
Bestimme VPN-Fähigkeits-Erkennungsinformation (VCDI)
202
200
VCDI an PEs ankündigen
204
Tunnel zwischen nahegelegenem PE und fernem PE unter Verwendung von VCDI konstruieren
206

Fig. 2

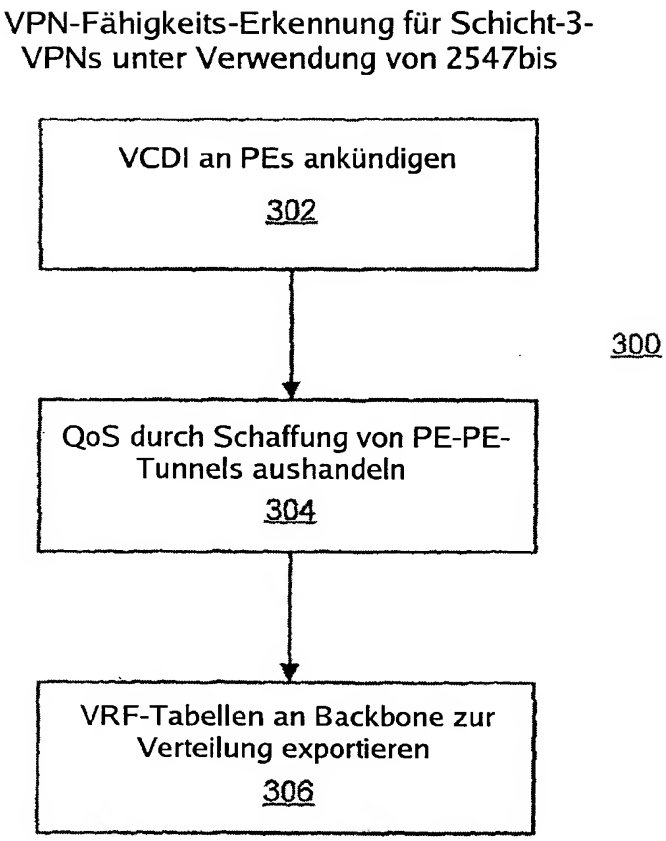
VPN-Fähigkeits-Erkennung für Schicht-3-VPNs unter Verwendung von 2547bis
VCDI an PEs ankündigen
302
300
QoS durch Schaffung von PE-PE-Tunnels aushandeln
304
VRF-Tabellen an Backbone zur Verteilung exportieren
306

Fig. 3

VPN-Fähigkeits-Erkennung für Schicht-3
VPNs unter Verwendung der virtuellen Routenführung

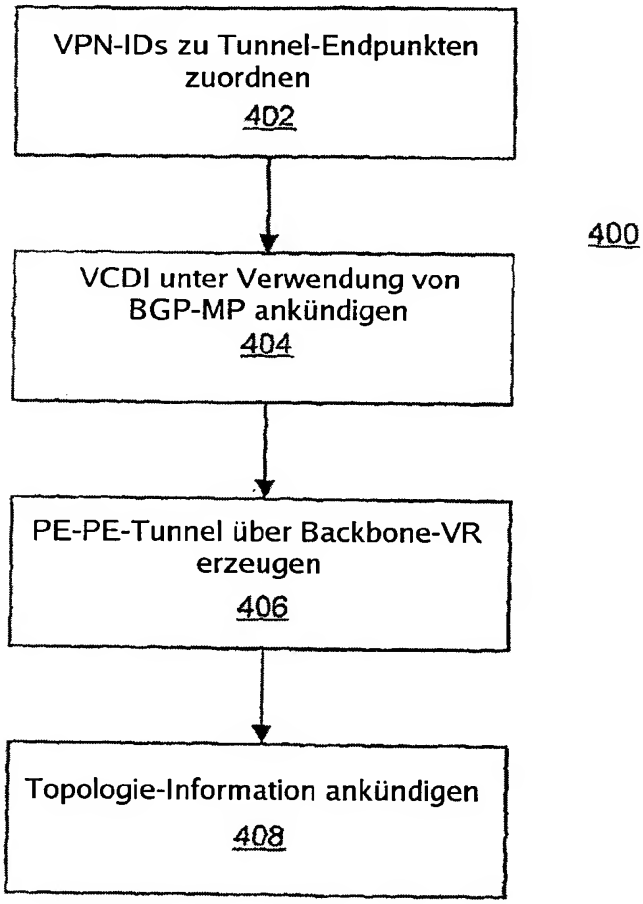

FIG. 4

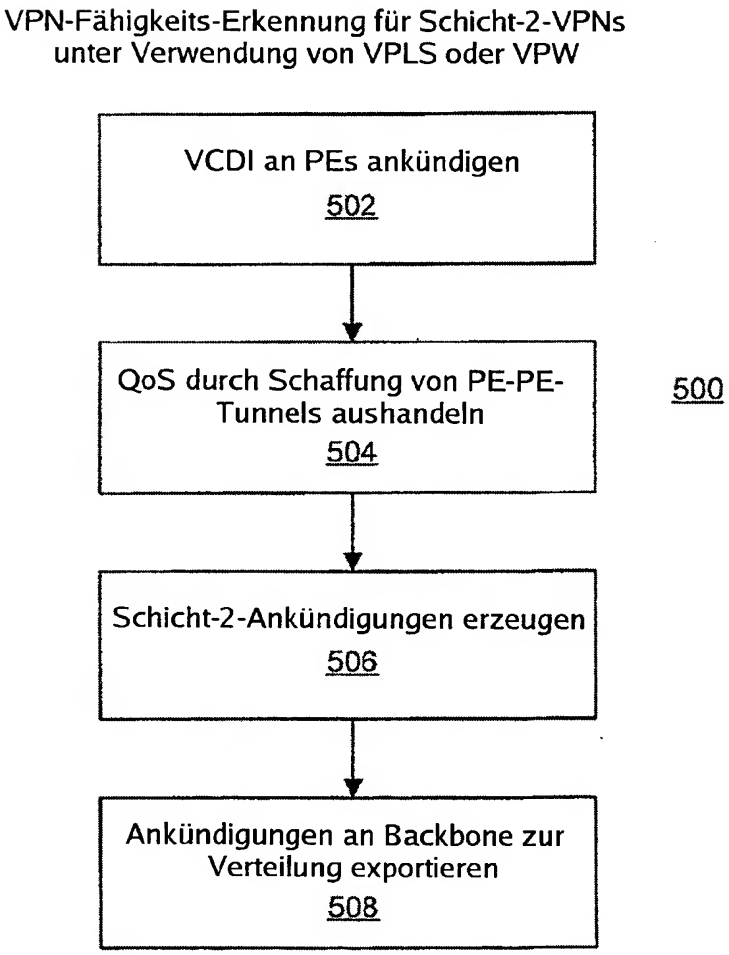
VPN-Fähigkeits-Erkennung für Schicht-2-VPNs unter Verwendung von VPLS oder VPW
VCDI an PEs ankündigen
502
QoS durch Schaffung von PE-PE-Tunnels aushandeln
504
500
Schicht-2-Ankündigungen erzeugen
506
Ankündigungen an Backbone zur Verteilung exportieren
508

Fig. 5